Docket No.: 62807-143 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Yoshimitsu NAMIOKA, et al.	:	Confirmation Number: 5406
Serial No.: 10/671,874	:	Group Art Unit: 2154
Filed: September 29, 2003	:	Examiner: Unknown

For: DATA COMMUNICATION METHOD AND INFORMATION PROCESSING APPARATUS FOR ACKNOWLEDGING SIGNAL RECEPTION BY USING LOW-LAYER PROTOCOL

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

At the time the above application was filed, priority was claimed based on the following application:

Japanese Patent Application No. 2002-284712, filed September 30, 2002

A copy of the priority application listed above is enclosed.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 KEG:tlb
Facsimile: (202) 756-8087
Date: January 9, 2004

G2807-143
NAMIOKA et al.
September 29, 2003

日本国特許庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　９月３０日

出願番号
Application Number: 特願２００２－２８４７１２

[ST. 10/C]: [ＪＰ２００２－２８４７１２]

出願人
Applicant(s): 株式会社日立製作所

２００３年１０月　７日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０８２４４０

【書類名】　特許願
【整理番号】　1102014801
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 11/00
【発明の名称】　データ通信方法および情報処理装置
【請求項の数】　12
【発明者】
【住所又は居所】　茨城県日立市大みか町五丁目２番１号
株式会社　日立製作所　情報制御システム事業部内
【氏名】　浪岡　良光
【発明者】
【住所又は居所】　茨城県日立市大みか町五丁目２番１号
株式会社　日立製作所　情報制御システム事業部内
【氏名】　宮尾　健
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社　日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【電話番号】　03-3212-1111
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　データ通信方法および情報処理装置

【特許請求の範囲】

【請求項１】

第２の計算機から第１の計算機へのデータ送信が制限されるプロトコルにより、前記第１の計算機から前記第２の計算機にデータ送信するステップと、

前記データ送信プロトコルよりも低層のプロトコルによって、前記第２の計算機から前記第１の計算機へ、前記第２の計算機でのデータ受信を示す信号を送信するステップを有するデータ通信方法。

【請求項２】

請求項１において、前記第２の計算機から前記第１の計算機へのデータ送信の制限は、物理層でなされるデータ通信方法。

【請求項３】

請求項２において、前記第２の計算機でのデータ受信を示す信号は、前記第１の計算機から前記第２の計算機にデータ送信する信号線とは物理的に異なる信号線として形成されているデータ通信方法。

【請求項４】

請求項３において、前記第２の計算機でのデータ受信を示す信号は、電圧或いは電流の変化で示されるデータ通信方法。

【請求項５】

請求項４において、前記第２の計算機から前記第１の計算機へのデータ送信の制限は、第２の計算機システムから第１の計算機システムにデータを送信するための通信線を排除したことによってなされるデータ通信方法。

【請求項６】

第２の計算機に対してデータ送信を送信するデータ送信処理部と、前記第２の計算機でデータ受信されたことを示す信号を入力する入力部を有し、前記第２の計算機からのデータ受信を制限する情報処理装置であって、前記データ送信プロトコルよりも低層のプロトコルによって、前記第２の計算機でのデータ受信を示す信号が前記入力部に入力されることを特徴とする情報処理装置。

【請求項７】

請求項６において、前記入力部は電気接点部であり、前記第１の計算機から前記第２の計算機に対して物理的に片方向のみ通信が可能な通信線により接続されていることを特徴とする情報処理装置。

【請求項８】

請求項７において、前記第１の計算機と前記第２の計算機を接続する通信線より、第２の計算機から第１の計算機にデータを送信するための通信線を排除し、前記第２の計算機から第１の計算機に対してはデータが送信されないことを特徴とする情報処理装置。

【請求項９】

請求項８において、前記第１の計算機と前記第２の計算機を接続する通信線を用いて、前記第１の計算機から前記第２の計算機にのみ片方向にデータを送信することを特徴とする情報処理装置。

【請求項１０】

請求項７において、前記電気接点部は、前記第２の計算機でデータを受信した情報を受け取るための接点であることを特徴とする情報処理装置。

【請求項１１】

請求項１０において、前記第１の計算機から前記第２の計算機にデータを送信する際に、前記電気接点で受信確認を行いながら通信することを特徴とする情報処理装置。

【請求項１２】

請求項６において、前記データ送信処理部から送信されるデータに送信回数を付与されており、ポート番号に従って受信すべき受信アプリケーションにデータが転送される情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信接続された計算機間におけるデータ通信方法、および、情報処理装置に関する。

【０００２】

【従来の技術】

従来、インターネットに代表されるネットワークシステムでは、相互のシステム保護や運用管理を目的として、ルータやファイアウォールと呼ばれるデータ通信装置を計算機間の通信路上に設置して、保護する第１の計算機システムから第２の計算機システムへの通信は許可し、反対に第２の計算機システムから第１の計算機システムへの通信を拒否する制御をソフトウェアによって論理的に実現していた（例えば、特許文献１）。

【０００３】

第１の計算機システムの振る舞いは正当なものであるという前提のもと、一般に広く用いられているＵＤＰ通信を制御する場合は、データ通信装置はパケットの内容を判定して、第１の計算機システムから第２の計算機システムへ送信した通信パケットであれば通信を許可し、反対に第２の計算機システムから第１の計算機システムへ送信した通信パケットは拒否する。

【０００４】

また、ＵＤＰ通信と同様に一般に広く用いられているＴＣＰ通信を制御する場合は、通信開始時のコネクション要求送信側が第１の計算機システムであれば通信を許可し、確立されたコネクションの中で以降に発生する、第１の計算機システムから第２の計算機システムへ送信したパケットだけでなく、ＴＣＰ通信を成立させるために用いられている、第２の計算機システムから第１の計算機にシステムへ送信したデータ受信応答パケットやコネクション切断パケットも許可する。反対に、コネクション要求送信側が第２の計算機システムであれば、データ通信装置はその要求を拒否する。

【０００５】

さらに最も安全な方式としては、計算機システム間をネットワークで接続せず、第１の計算機システムにあるデータを外部記憶媒体に保存し、人間の手作業により第２の計算機システムへ転写することもある。

【０００６】

【特許文献１】

特開２０００－１５６７１１号公報

【０００７】

【発明が解決しようとする課題】

従来技術で実現されたルータやファイアウォールなどのデータ通信装置を、第１の計算機システムから第２の計算機システムの間に設置して、第１の計算機システムから第２の計算機システムへ論理的な片方向通信を実現した場合でも、実際には通信線が双方向通信できる状態にあるため、論理の定義や環境設定の定義が誤っていると、双方向通信が可能となってしまい、結果的にネットワーク経由での不正侵入が可能となる場合がある。

【０００８】

また、不正侵入された第２の計算機システムから、パケットの送信先が第１の計算機システムであると不正に偽造されたパケットをデータ通信装置に送信すると、第１の計算機システムへ送信することが可能となる。その場合、第２の計算機システム上で不正に作成・実行された攻撃用プログラムを実行することによって、第１の計算機システムに対してデータ通信装置を越えてパケットを大量に送信し、第１の計算機システムの動作を著しく妨害する攻撃が可能になることが知られている。

【０００９】

このように、論理的に片方向通信となるようにした場合でも、本来はデータを送信できないはずの第２の計算機システムから第１の計算機システムに向けた通信路が物理的に存在する場合は、第１の計算機が攻撃されてしまう可能性が残っており、かつデータを送信できた場合は、その行為自体が攻撃になりうることが問題であった。

【００１０】

本発明の目的は、仮想的な計算機への攻撃に対して、安全性の高いものを提供することにある。

【００１１】

【課題を解決するための手段】

上記目的を達成するために、第１の計算機から第２の計算機にデータ送信し、

第２の計算機から第１の計算機へ、第２の計算機でのデータ受信を確認信号を送信し、第２の計算機から第１の計算機へのデータ送信は制限され、より低層のプロトコルによって、第２の計算機での信号受信の確認をなすように構成した。

【００１２】

【発明の実施の形態】

図１は、本発明の実施例を示す実施例１のブロック図である。計算機（１０１）が保持するデータを、通信線（３０１）で接続された計算機（２０１）へ片方向に送信する場合の構成であり、データの送信元となる計算機（１０１）にはデータ送信処理部（１０２）と電気接点入力部（１０３）を実装し、データを受信する計算機（２０１）には、データ受信処理部（２０２）と電気接点出力部(203)を実装する。また、計算機（１０１）と計算機（２０１）の間で電気接点入力部（１０３）と電気接点出力部（２０３）を電線（或いは、単に通信線と称する）（６０１）で接続することで、データ通信装置（９０１）が構成される。ここで、データ送信処理部（１０２）はデータ受信処理部（２０２）に向けてデータを送信（７１０）し、データを受信したデータ受信処理部（２０２）は電気接点出力部（なお、電気接点出力部と電気接点入力部を総称して単に電気接点と称する。）に接点出力（７２０）を行う。電気接点出力部(２０３）は、電線(６０１）にかかる電圧あるいは電流を変化させることにより電気接点入力部（１０３）へ受信の完了を伝達する（７３０）。例えば、電気接点入力部（１０３）において、所定の電流より高くなったとき、或いは、所定の電圧よりも高くなったときに、電気接点出力部（２０３）から信号が発せられたと検出する。このような、以下に説明するＩＥＥＥ８０２．３で規定されるプロトコルと比較すると、下位であり、物理層に近い層を利用して通信を行う。

【００１３】

接点の変化を検知した電気接点入力部（１０３）は、受信の完了をデータ送信処理部（１０２）へ報告する(７４０）。このように、電気接点出力部(２０３）と電気接点入力部（１０３）は、電線（６０１）によって結ばれている。この電線（６０１）は通信線（３０１）とは物理的に異なる線で構成されている。

【００１４】

図１における通信線（３０１）の信号線を物理的に片方向通信のみとした構成を図２で説明する。一般のＩＥＥＥ８０２．３の１０ＢＡＳＥ－Ｔに準拠した通信線は、電気的に正負の電線を対で持ち、それを２組用意することで双方向通信を実現している。すなわち、通信プロトコルとしては、物理層，データリンク層，ネットワーク層を有しおり、これらより上位の層を利用してデータの授受を行う。

【００１５】

そこで、通信線（３０１）の、送信側のコネクタ（４１１）と受信側コネクタ（４２１）にある電線の接続を変更する。一般に、双方向通信を行うためには、電気的にデータ送信側の端子ＴＸ＋～データ受信側のＲＸ＋、データ受信側のＴＸ－とデータ送信側のＲＸ－を接続した対の電線が双方向必要となり、２対用意することになるが、送信側コネクタ（４１１）ＲＸ＋（４１１－３）と受信側コネクタ(４２１）ＲＸ＋(４２１－３）を結ぶ電線に、送信側コネクタ(４１１）ＴＸ＋（４１１－１）の電線を接続し、さらに送信側コネクタ（４１１）ＲＸ－（４１１－４）と受信側コネクタ（４２１）ＲＸ－（４２１－４）を結ぶ電線に、送信側コネクタ（４１１）ＴＸ＋（４１１－２）の電線を接続する。結果、受信側コネクタ（４２１）のＴＸ＋（４２１－１）～送信側コネクタ（４１１）のＲＸ＋（４１１－３）、および送信側コネクタ（４１１）のＴＸ－(４１１－２）～受信側コネクタ（４２１）のＲＸ－（４２１－４）の通信経路が無くなったことにより、受信側コネクタから送信側コネクタへのデータ送信は物理的に不可能になる。つまり、計算機（２０１）側となる受信側コネクタＴＸ＋(４２１－１）およびＴＸ－（４２１－２）の電線を排除することによって、計算機（２０１）から計算機（１０１）に対しては物理的に通信できない状態とし、反対に計算機（１０１）から計算機（２０１）に対しては片方向の通信が可能となる。片方向の通信を行うために、コネクタの電線を物理的に排除することもプロトコルに含まれると定義される。

【００１６】

また、物理的な接続状態を監視する信号リンクテスト・パルスを用いて異常を検知する仕組みがＩＥＥＥ８０２．３で規定されているため、一般の通信装置で

はＴＸ＋およびＴＸ－あるいはＲＸ＋およびＲＸ－の電線を排除した通信線を用いた場合には、通信相手から受け取るはずのリンクテスト・パルスを検知できず、通信することができない。本発明では、送信側のＴＸ＋（４１１－１）をＲＸ＋（４１１－３）、送信側のＴＸ－（４１１－２）をＲＸ－（４１１－４）に接続してリンクテスト・パルスを強制的に有効にしたことにより、通信を可能とした。

【００１７】

図１における通信方式を図３で説明する。まず、データ受信処理部（２２０）は、受信アプリケーション（２１０）が規定のポート番号で通信可能な状態にしたソケットを受け取り（２１１）、該ソケットを用いて、データ受信待ち状態に入る（２２１）。

【００１８】

ここで、データ送信処理部（１２０）は、通信可能な状態のソケットとデータを送信アプリケーション（１１０）から受け取り（１１１）、既知の技術である一方向通信方式ＵＤＰなどを用いて送信（１２１）し、接点入力待ち状態に入る（１２２）。接点入力待ち状態（１２２）は、接点出力時における接点入力検出までの時間より長いタイムアウト時間を閾値として設定し、タイムアウト時間を超過した場合、もしくは接点入力を検知した場合に待ち状態を解除する。データ受信処理部（２２０）は、データ送信処理部（１２０）から送信（１２１）されたデータを受信したならば、受信確認の応答を意味する接点出力（２２２）を行い、受信したデータを受信アプリケーション（２１０）に返す（２１２）。なお、データ送信処理部（１２０）が送信アプリケーション（１１０）から受け取る情報は、ソケットとデータの他、送信すべきデータ量などを加えてもよい。また、データ受信処理部（２２０）が受信アプリケーション（２１０）に返す情報は、受信データの他、受信したデータ量やエラーコードを加えてもよい。

【００１９】

次に、データ送信処理部（１２０）が受信確認の応答を意味する接点入力を検知した場合は、接点入力待ち状態（１２２）を解除する。そこで解除の要因を調べ（１２３）、解除の要因がタイムアウト時間の超過にあるならば再送を試みる

ものとし、現在の試行回数を調べる（１２４）。規定の試行回数を超過していなければ再度データを送信（１２１）し、規定の試行回数を超過した場合は再送を行わず、送信アプリケーション（１１０）にエラーを意味するエラーコード（１１２）を返して終了する。あるいは、解除の要因が接点入力だったならば、送信アプリケーション（１１０）に送信データのサイズを返して処理を終了し、データの送信を完了する。このとき、エラーコードの代わりに送信したデータ量を返してもよい。

【００２０】

本発明の実施例２として、図３で説明した通信方式を応用し、複数アプリケーションで通信が可能となる通信方式を図４で説明する。通信を行う前に、送信アプリケーション（１１０）とデータ受信処理部（２２０）は相互に、アプリケーションとポート番号を対にした、ポート番号一覧（２３０）を認識しているものとし、複数の受信アプリケーション（２１０）が規定のポート番号で受信待ちを行うものとする。さらに、受信アプリケーション（２１０）は、ポート番号一覧（２３０）で示されたポート番号でデータの受信待ちを行うものとする。

【００２１】

ここで、データ送信処理部（１２０）は、送信アプリケーション（１１０）からデータの送信要求があった場合、他の送信アプリケーションからの送信要求を排他した状態で、ソケットとデータに加えてポート番号を受け取り、データ（７１０－２）の先頭にポート番号（７１０－１）を付与して計算機（２０１）のデータ受信処理部（２２０）に送信する。データ受信処理部（２２０）は、受信したデータをポート番号（７１０－１）とデータ（７１０－２）に分解し、抽出したポート番号で受信待ちを行っている受信アプリケーション（２１０）に対してデータを転送した後、接点出力（２２０－２）を行う。接点入力待ち状態になっていたデータ送信処理部（１２０）は、接点入力を検出したならば送信を完了し、送信要求の排他状態を解除して、他の送信アプリケーションからの送信要求を受付可能とする。

【００２２】

なお、データ送信処理部（１２０）とデータ受信処理部（２２０）、およびそ

れらの間で用いる接点を複数用意してもよい。また、送信するデータには、ポート番号（７１０－１），データ（７１０－２）の他にデータのサイズなどの管理情報を含めてもよい。

【００２３】

本発明の実施例３として、接点による応答回数を減らすことにより送信効率を向上させた通信方式を図５で説明する。まず、計算機（１０１）のデータ送信処理部（１２０）は、送信アプリケーション（１１０）からソケットとデータ、およびデータサイズに加え、送信回数とデータ番号を受け取り、送信データとして送信回数（７１０－１）、データ番号（７１０－２）、データ（７１０－３）を送信する。このとき、データサイズを含めてもよい。データ送信処理部(１２０)は、送信アプリケーション（１１０）から、データ番号が増加もしくは減少しながら送信回数分だけ送信要求を受理するものとし、受理した送信回数分のデータを計算機（２０１）のデータ受信処理部（２２０）に送信する。送信したデータが最後のデータであれば、データ送信処理部（１２０）は接点入力待ち状態に入る。次に、データ受信処理部（２２０）は、受信した送信回数（７１０－１）の分だけデータ（７１０－３）を受信し、かつデータ番号（７１０－２）が重複や欠落がないことを確認した場合、受信アプリケーション（２１０）へデータを渡した後、接点出力を行う。接点入力待ち状態になっていたデータ送信処理部（１２０）は、規定のタイムアウト時間分を超過するか、あるいは接点入力を検知した場合に接点入力待ち状態を解除し、送信アプリケーションに送信成否を報告する。このとき、データ送信処理部（１２０）は、送信アプリケーション（１１０）に送信失敗を報告することにより、再送処理を促すことができる。

【００２４】

本発明の実施例４として、確実にデータが送信されたことを確認する必要がなければ、図１で示したデータ送信処理部（１０２）が接点による受信確認を行うことなくデータを送信しつづけてもよい。

【００２５】

総括的に説明すると、第１の計算機システムが保持するデータを第２の計算機システムへ送信することが可能だが、第２の計算機システムから第１の計算機シ

ステムにはデータを送信できないため、第１の計算機システムが保持するデータを、第２の計算機システムにて不特定多数の利用者に公開することができる。

【００２６】

また、第２の計算機が不正に侵入されてしまった場合であっても、物理的に第１の計算機システムと通信できないため、不正侵入や、大量のパケットを送信して計算機のサービスを妨害する攻撃を阻止することができる。

【００２７】

さらに、片方向通信でありながら、第１の計算機システムから第２の計算機システムにデータを送信する際、電気接点を用いて受信確認を行うことができるため、データを受信すべき第２の計算機システムが真にデータを受信したかどうかを確認し、受信していなければデータを再送することが可能となる。

【００２８】

【発明の効果】

以上説明したとおり、本発明によれば、仮想的な計算機への攻撃に対して、安全性の高いデータ通信方法或いは情報処理装置を得ることができる。

【図面の簡単な説明】

【図１】

本発明の構成図。

【図２】

ネットワーク回線の構成。

【図３】

計算機間の通信方式。

【図４】

複数の送受信アプリケーションに対応した通信方式。

【図５】

分割送信時の通信方式。

【符号の説明】

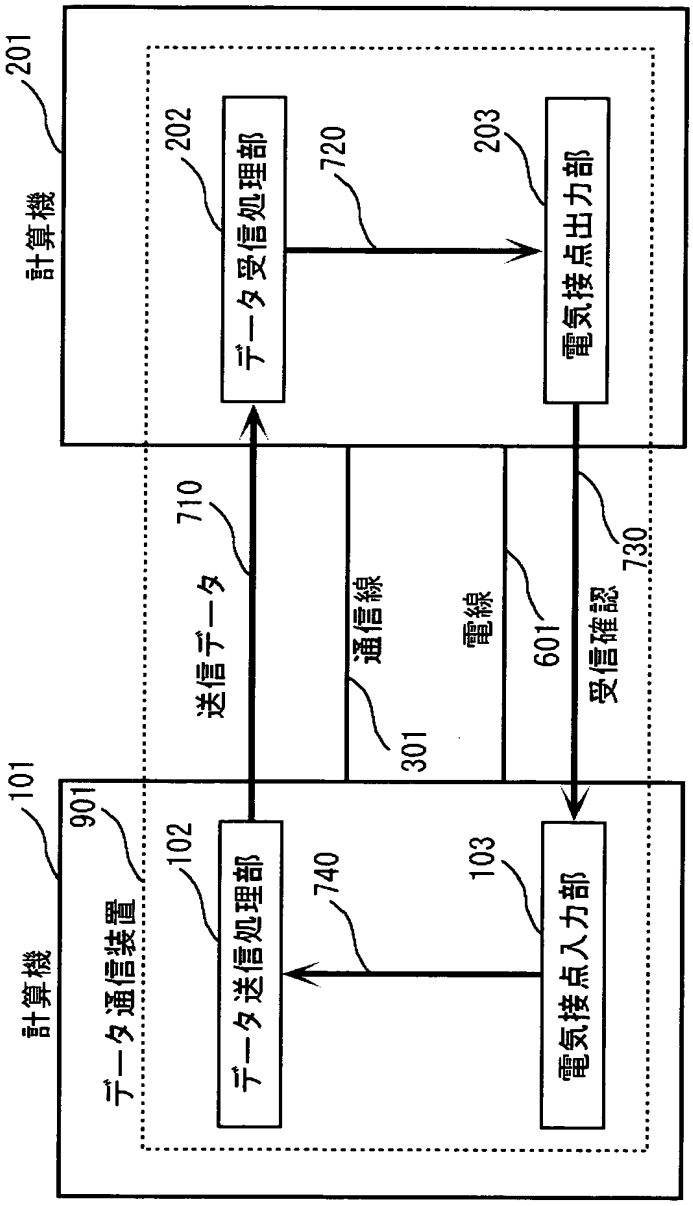
１０１，２０１…計算機、１０２…データ送信処理部、１０３…電気接点入力部、２０２…データ受信処理部、２０３…電気接点出力部、３０１…送信線、

６０１…電線。

【書類名】　図面

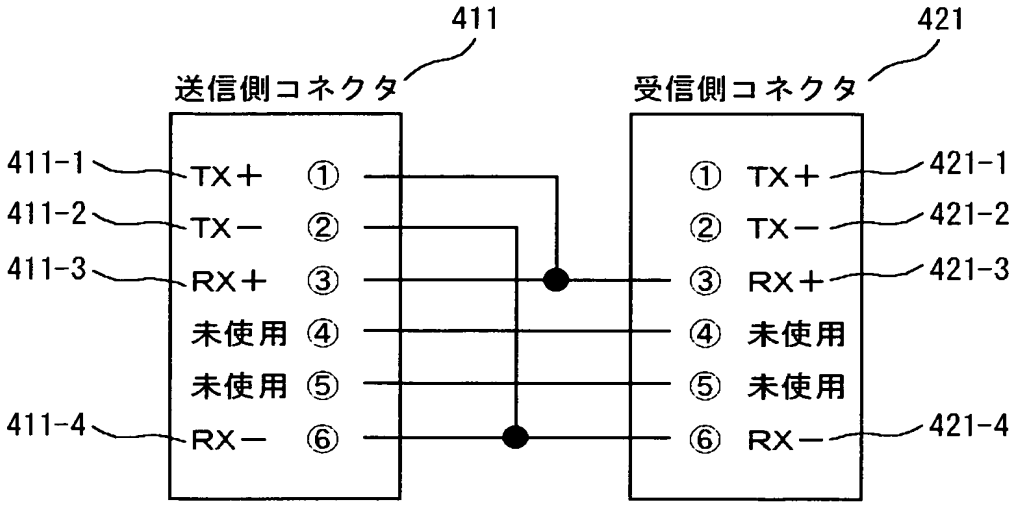
【図１】

図　1


201
計算機
202
データ受信処理部
720
203
電気接点出力部
710
送信データ
通信線
301
電線
601
受信確認
730
101
901
データ通信装置
102
データ送信処理部
740
103
電気接点入力部
計算機

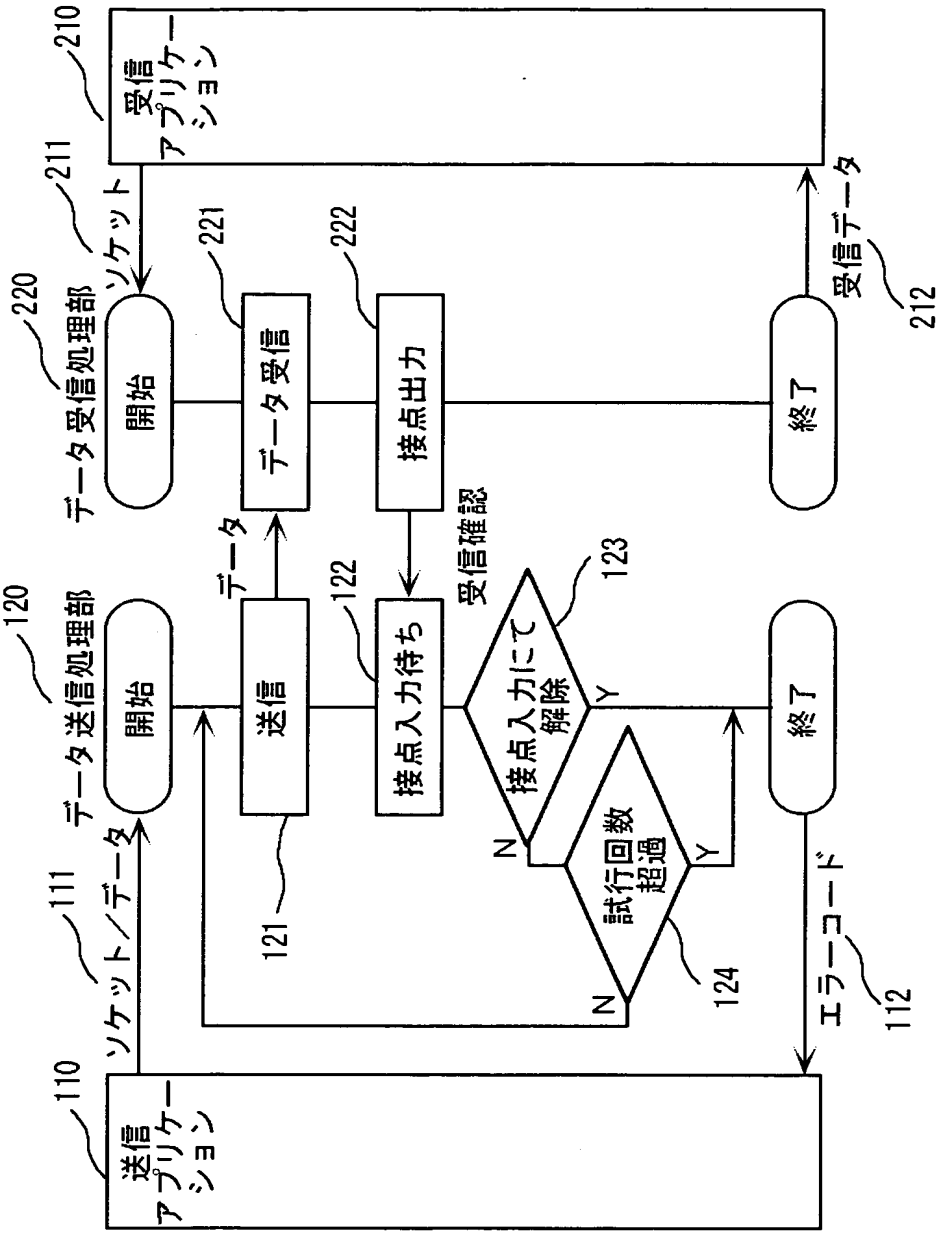
【図２】

図　２


411
送信側コネクタ
421
受信側コネクタ
411-1
411-2
411-3
411-4
TX＋ ①
TX－ ②
RX＋ ③
未使用 ④
未使用 ⑤
RX－ ⑥
① TX＋
② TX－
③ RX＋
④ 未使用
⑤ 未使用
⑥ RX－
421-1
421-2
421-3
421-4

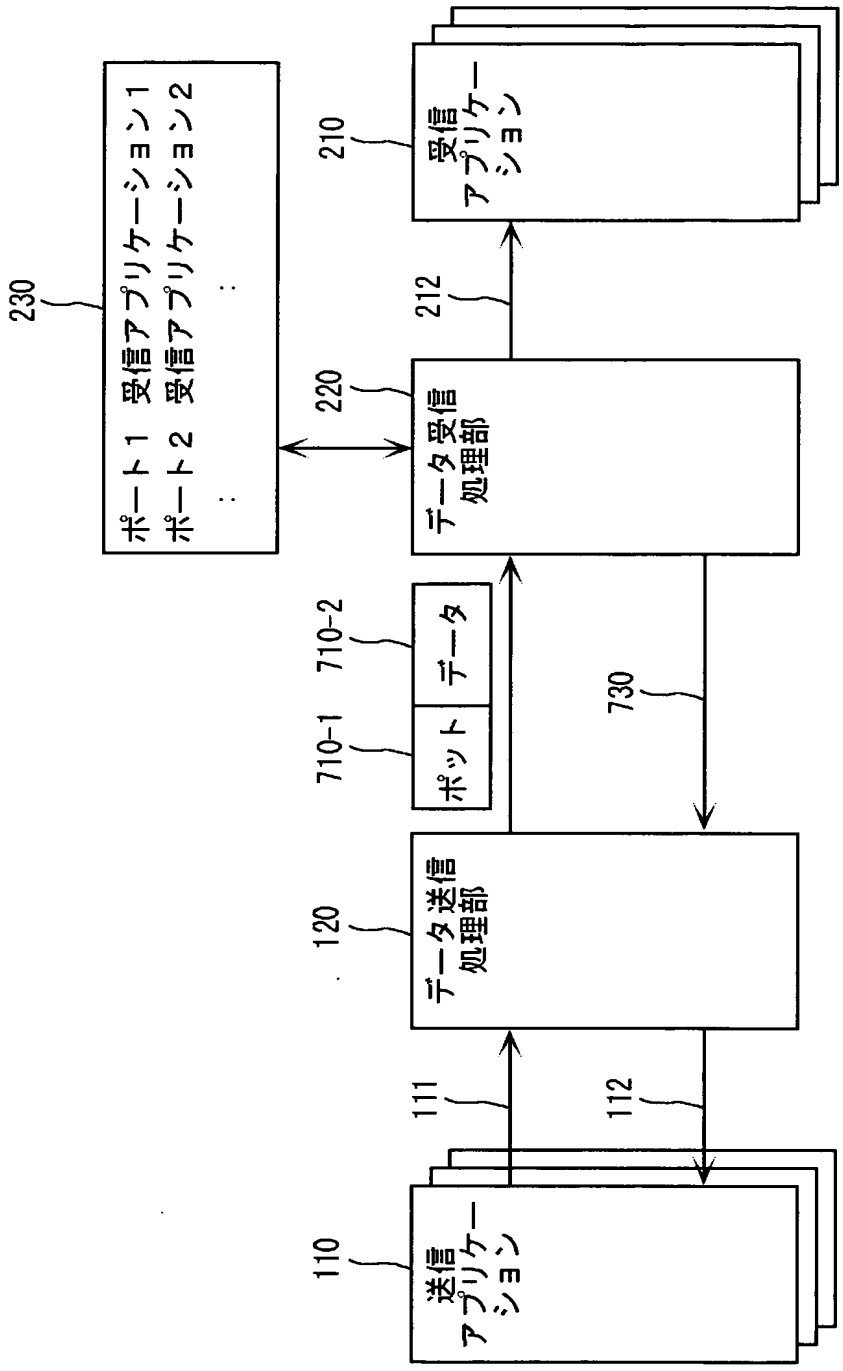
【図３】

図　３


受信アプリケーション
210
ソケット
211
データ受信処理部
220
開始
データ受信
221
接点出力
222
終了
受信データ
212
データ
受信確認
送信処理部
120
開始
送信
121
接点入力待ち
122
接点入力にて解除
123
Y
N
試行回数超過
124
Y
N
終了
ソケット／データ
111
エラーコード
112
送信アプリケーション
110

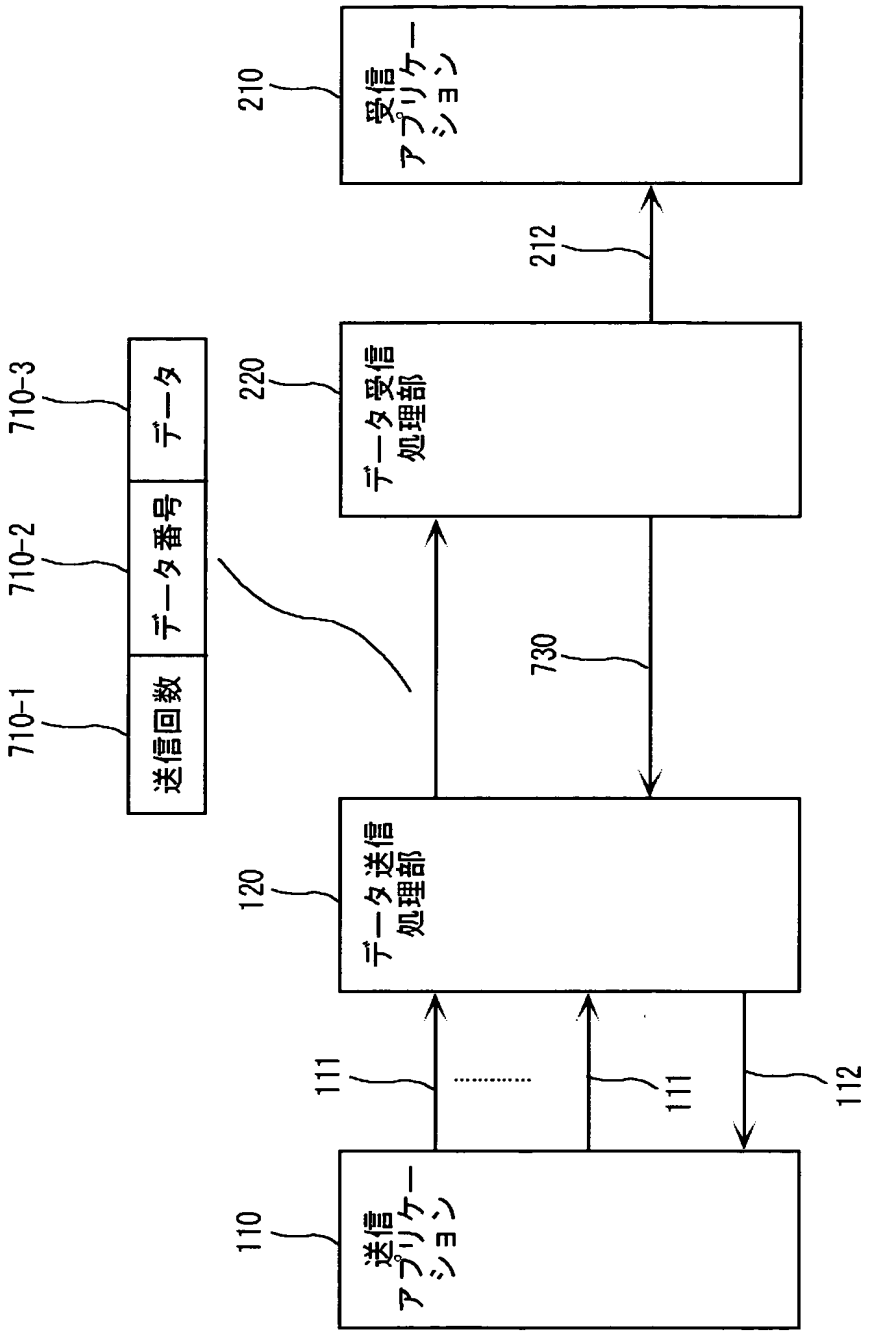
【図４】

図　４


ポート１ 受信アプリケーション１
ポート２ 受信アプリケーション２
230
210
受信アプリケーション
212
220
データ受信処理部
710-2
データ
710-1
ポット
730
120
データ送信処理部
111
112
110
送信アプリケーション

【図５】

図　５


受信アプリケーション
210
212
データ受信処理部
220
730
データ送信処理部
120
111
111
112
送信アプリケーション
110
710-3
データ
710-2
データ番号
710-1
送信回数

【書類名】　要約書

【要約】

【課題】

従来はファイアウォール等で計算機への攻撃に対して防御していた、しかしながら、防御が十分でなく、高い安全性を得ることができなかった。

【解決手段】

上記課題に鑑み、第１の計算機から第２の計算機にデータ送信し、第２の計算機から第１の計算機へ、第２の計算機でのデータ受信を確認信号として送信し、第２の計算機から第１の計算機へのデータ送信は制限され、より低層のプロトコルによって、第２の計算機での信号受信の確認をなすように構成した。

【効果】

計算機への攻撃に対して、安全性の高いデータ通信方法或いは情報処理装置を得ることができる。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－２８４７１２
受付番号	５０２０１４５９１０２
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１４年１０月　１日

＜認定情報・付加情報＞

【提出日】　平成14年 9月30日

次頁無

出証特２００３－３０８２４４０

特願２００２－２８４７１２

出　願　人　履　歴　情　報

識別番号　　［０００００５１０８］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所